NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

NASES Bratislava
Trnavská cesta 100
821 01 Bratislava 2

Váš list číslo/zo dňa	Naše číslo	Vybavuje	Bratislava
07. 12. 2017	08805/2017/KÚ/OLP-002	odbor legislatívy a práva	15. 12. 2017

Vec
Odpoveď na: Žiadosť o usmernenie - spôsob vyhodnocovania QTS a QES

Národnému bezpečnostnému úradu (ďalej len „úrad“) bola dňa 11.12.2017 doručená žiadosť Vaša žiadosť o metodické usmernenie k nasledujúcim okruhom otázok:

- Spôsob vyhodnocovania platnosti certifikátu časovej pečiatky.
- Spôsob validácie kvalifikovaných elektronických podpisov a pečatí s neplatnými časovými pečiatkami.
- Spôsob vyhodnocovania platnosti autorizácie vo formátoch XAdES_ZEP a ZEPf (CAdES_ZEP).

Úrad v súvislosti s predmetnou žiadosťou odporúča postupovať podľa nasledovných usmernení k jednotlivým otázkam:

- *Spôsob vyhodnocovania platnosti certifikátu časovej pečiatky*
Ak je certifikát časovej pečiatky zverejnený v Dôveryhodnom zozname (http://ep.nbu.gov.sk/kca/tsljtsl.xml) so statusom "Granted" (t. j. v nasledovnej forme: http://uri.etsi.org/TrstSvc/Trustedlist/Svcstatus/granted) musí byť vždy považovaný za platný? Platí to aj v prípade, ak už uplynul dátum konca platnosti uvedený v tomto certifikáte?

Áno, čas uvedený v certifikáte je upravený v § 6 ods. 2 písm. c) zákona č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách), kde sa upravuje postup pre interval použitia súkromného kľúča služby s kvalifikovaným štatútom uvedenom v dôveryhodnom zozname (ďalej len „TL“). Používanie súkromného kľúča v intervale zjednotenia intervalov z certifikátov danej služby z TL podľa Validity intervalu (notBefore Time, notAfter Time) certifikátu, kde je tento interval možné skrátiť uvedením rozšírenia TL po nahlásení požiadavky orgánu dohľadu o skrátenie použitia privátneho kľúča. Pri koreňovej hierarchickej X.509 validácii si subjekt certifikátu dohodne s vydavateľom certifikátu dobu (Validity interval), počas ktorej je mu poskytnutá služba možného zrušenia platnosti, ak napr. dôjde k zmene údajov v certifikáte, alebo kompromitácii kľúča. Po tejto dobe (Validity interval) sa už služba nahlásenia zrušenia a jeho zverejnenia v CRL alebo v OCSP odpovedi neposkytuje. Ak je certifikát priamo v TL, (Validity interval) je doba použitia súkromného kľúča, pričom časový interval, počas ktorého je možné zmeniť platnosť služby, je určený kvalifikovaným stavom služby, ktorý sa môže odobrať a validácia služby je tak neplatná. Služba má kvalifikovaný štatút aj po čase, kedy sa už súkromný kľúč služby nesmie použiť a v tomto období poskytuje informácie o stave vydaných certifikátov,

pečiatok alebo iných výstupov svojej služby pre dlhodobé použitie a minimálne vedie tieto informácie 10 rokov aj po ukončení použitia súkromného kľúča.

Musia byť vydané kvalifikované časové pečiatky považované za platné až do času, kým sa v uvedenom Dôveryhodnom zozname zmení status certifikátu týchto časových pečiatok z "Granted" na status "Withdrawn", prípadne iný?

Áno, stav v TL je pre službu a nie pre certifikát. Certifikát v TL je len úložisko verejného kľúča služby, názvu služby a intervalu použitia súkromného kľúča služby (§ 6 ods. 2 zákona o dôveryhodných službách), kedy po uplynutí alebo skrátení intervalu sa musia zničiť všetky kópie súkromného kľúča, aby nedošlo k falošným spätným odpovediam.

Bude sa v Dôveryhodnom zozname (http://ep.nbu.gov.sk/kca/tsl/tsl.xml) meniť status certifikátu časovej pečiatky na základe skutočnosti, že uplynie dátum konca platnosti tohto certifikátu?

Nie, stav udelenia kvalifikovaného štatútu trvá aj po ukončení (Validity intervalu) certifikátu (napríklad 10 rokov je poskytovateľ služby povinný viesť dokumentáciu a je povinný podrobiť sa auditu a dohľadu).

Bude sa v Dôveryhodnom zozname (http://ep.nbu.gov.sk/kca/tsl/tsl.xml) meniť status certifikátu časovej pečiatky hneď po uplynutí dátumu konca platnosti tohto certifikátu? Ak nie, tak s akým časovom odstupom k zmene statusu príde?

Nie, pokiaľ nenastane bezpečnostný incident alebo nezhoda s požiadavkami na poskytovanie služby, alebo pokiaľ poskytovateľ nepožiada o zrušenie kvalifikovaného štatútu.

Na základe akých údajov je možné vopred očakávať konkrétny dátum zmeny statusu certifikátu časovej pečiatky v Dôveryhodnom zozname po uplynutí dátumu konca platnosti tohto certifikátu? Poznámka: Takýto dátum je potrebné vopred vedieť odhadnúť z dôvodu potreby prepečiatkovania.

Takýto čas nie je určený. Pri hierarchickej X.509 tiež nie je dopredu určený a certifikát môže byť zrušený kedykoľvek počas (Validity intervalu) certifikátu časovej pečiatky, a teda spoliehať sa na (Validity interval) certifikátu časovej pečiatky nie je ani možné ani ak je certifikát priamo uvedený v TL. Čas, kedy je vhodné opätovne časovo pečiatkovať údaje je daný na základe analýzy rizík.

V prípade, že sa nebude prihliadať pri overovaní elektronických podpisov a pečatí na dátum ukončenia platnosti certifikátu časovej pečiatky (certifikát časovej pečiatky sa bude považovať za platný, ak bude zverejnený v Dôveryhodnom zozname so statusom "Granted") akým spôsobom bude zabezpečená dlhodobá overiteľnosť tak, aby v prípade neočakávanej zmeny stavu certifikátu (napr. diskreditácia privátneho kľúča) nenastala situácia, ktorá spôsobí nemožnosť overenia platnosti certifikátu časovej pečiatky a tým aj všetkých elektronických podpisov a pečatí, ktoré ju obsahujú?

Služba časovej pečiatky musí po (Validity intervale) z certifikátov v TL služby nenávratne zničiť kópie súkromného kľúča. Ak dôjde ku kompromitácii aj napriek tomuto zničeniu kľúčov, je to rovnaká situácia ako pri hierarchickom X.509 validovaní – je potrebná analýza rizík.

- <u>Spôsob validácie kvalifikovaných elektronických podpisov a pečatí s neplatnými časovými pečiatkami</u>

V prípade že kvalifikovaný elektronický podpis/pečať má pripojenú jedinú kvalifikovanú časovú pečiatku, ktorej certifikát je neplatný (viď bod 1), musí sa pri overení podpisu/pečate vyhodnocovať platnosť tohto podpisu/pečate nezávisle od časovej pečiatky (t. j. rovnakým spôsobom ako keby žiadna časová pečiatka pripojená nebola?)?

Áno, rôzne subjekty môžu používať rôzne časové pečiatky s rôznou dôverou v ich bezpečnosť a ich počet nie je obmedzený. Najstaršia platná časová pečiatka, pre prostredie spoliehajúcej sa strany, je použitá na určenie času, ku ktorému sa validácia vykoná. Ak nie je žiadna časová pečiatka platná, podpis dokumentu sa overuje k aktuálnemu času a ak nie je certifikát podpisovateľa v CRL alebo v OCSP odpovedi zrušený, oznámi sa že k dátumu a času z položky *thisUpadat* z CRL alebo OCSP odpovede je podpis alebo pečať platná.

Platí uvedené pravidlo rovnako pre všetky formáty podpisov/pečatí v zmysle Vykonávacieho rozhodnutia 2015/1506 - t. j. CAdES Baseline Profile, XAdES Baseline Profile, PAdES Baseline Profile, ASiC Baseline Profile? Poznámka: Pýtame sa z dôvodu, že dodávateľ dodal riešenie, kedy sa v prípade podpisu/pečate XAdES Baseline Profile s neplatnou časovou pečiatkou vyhodnocuje podpis/pečať rovnako akoby časovú pečiatku nemal. Avšak v prípade CAdES Baseline Profile s neplatnou časovou pečiatkou sa už podpis/pečať nevyhodnocuje a výsledkom overenia je vždy neplatná autorizácia.

Áno platí to rovnako pre všetky formáty.

- <u>Spôsob vyhodnocovania platnosti autorizácie vo formátoch XAdES_ZEP a ZEPf (CAdES_ZEP)</u>

Sú pôvodné formáty XAdES_ZEP a ZEPf (CAdES_ZEP) v súlade s Nariadením EP a Rady (EÚ) č. 910/2014 (ďalej aj ako „Nariadenie")? Je možné tieto profily používať za účelom vykonania autorizácie elektronických dokumentov, resp. ak áno, tak do akého času ich je možné využívať?

Formát podpisu XAdES_ZEP je vo verzii od 1 do 2 a jeho rozšírenia majú požiadavky nad rámec požiadaviek prílohy Vykonávacieho rozhodnutia Komisie č. 2015/1506, z tohto dôvodu sa nemôže vyžadovať ich plnenie. Formát podpisu ZEPf (CAdES_ZEP) je CAdES podpis EML dokumentu uložený v ZIP s premenovanou koncovkou na ZEP, čo znamená, že je v súlade s prílohou Vykonávacieho rozhodnutia Komisie č. 2015/1506 a je ho možné validovať ako samostatný CAdES dokumentu EML, alebo vložiť do ASiC a validovať ako ASiC v súlade s nariadením Európskeho parlamentu a Rady č. 910/2014.

Je povinnosť zo strany orgánov verejnej moci prijímať ZEPf, resp. podpis v ZEPf (CAdES_ZEP)?

Podpis áno. Dokument EML je e-mail s dokumentom v prílohe e-mailu v base64 kódovaní. ZEPf je len transportný formát pre podpis a podpísaný elektronický dokument. Nejde o formát podpisu a nedefinuje obmedzenia a ani požiadavky na obsah CAdES a XAdES, ktorý môže byť v ZEPf transportovaný.

Rovnako je povinnosť zo strany orgánov verejnej moci prijímať XAdES_ZEP?

Nie, lebo formát má požiadavky nad rámec požiadaviek prílohy Vykonávacieho rozhodnutia Komisie č. 2015/1506.

Overovanie platnosti autorizácie v týchto formátoch je v súčasnosti realizované podľa pravidiel definovaných v profiloch pre XAdES_ZEP a ZEPf (CAdES_ZEP). Je možné zmeniť spôsob overovania platnosti autorizácie, ak by táto zmena bola v rozpore s pravidlami definovanými v týchto profiloch? Obávame sa totiž, že by mohla v praxi nastať situácia, kedy by výsledok overenia podpisu v minulosti bol iný ako výsledok získaný po aplikovaní tejto zmeny v overovaní, čo by mohlo vyvolať prípadné spory a stav neistoty. Poznámka: V súčasnosti stále prevláda situácia, keď sú prostredníctvom rezortných podateľní a ÚPVS (CEP) vytvárané, spracovávané a vyhodnocované formáty podpisov/pečatí: XAdES_ZEP a ZEPf(CAdES_ZEP), ktorých je pochybnosť, čii sú v súlade s Nariadením EP a Rady (EÚ) č. 910/2014.

Odpoveď na otázku je obsiahnutá v texte vyššie. V každom prípade je potrebné rozlišovať validovanie formátu podpisu a validovanie platnosti kvalifikovaného certifikátu. Validovanie certifikátu je podľa nariadenia Európskeho parlamentu a Rady č. 910/2014 zhodné s postupom s pred 1.7.2016, kedy bol TL len informatívny, ale ponúkal rovnaké výsledky a obsahuje preto históriu z pred 1.7.2016 pre umožnenie overenia, na základe ktorej sa overuje stav certifikátov z podpisov vyhotovených pred 1.7.2016 zhodne, a to podľa dostupnosti údajov v TL, v samotnom podpise a v službách ako OCSP a CRL, ktoré musia obsahovať aj stav pre expirované certifikáty. Validovanie formátu podpisu XAdES_ZEP, vyhotoveného po 01.07.2016 je nad rámec požiadaviek pre kvalifikovaný elektronický podpis, a preto je dobrovoľné a teda nie je povinné pre orgán verejnej moci ak akceptujú len kvalifikovaný elektronický podpis. Validovanie ZEPf (CAdES_ZEP) je po rozbalení z transportného ZIP zhodné s požiadavkami nariadenia Európskeho parlamentu a Rady č. 910/2014.

Na prechod a zavedenie používania výlučne iba nových formátov, ktoré sú v súlade s Nariadením je potrebná koordinácia všetkých orgánov verejnej moci a následné je možné sprístupnenie nových funkcionality CEP na ÚPVS. Aj po prechode na formáty súladné s Nariadením budú na ÚPVS v elektronických schránkach dostupné elektronické podania a elektronické úradné dokumenty autorizované formátmi podpisov podľa legislatívy platnej pred účinnosťou Nariadenia.

Vyhotovovanie je povolené pre orgány verejnej moci na základe prílohy Vykonávacieho rozhodnutia Komisie č. 2015/1506 a rovnako povinnosť ich akceptovať je len dobrovoľná, ak boli vyhotovené po 01.07.2016 a nie sú v súlade s prílohou Vykonávacieho rozhodnutia Komisie č. 2015/1506, ak orgán verejnej moci nedeklaruje, že prijíma aj bezpečnostne nižšie formáty, než je kvalifikovaný elektronický podpis. Je potrebné vziať primerane na vedomie § 23 ods. 1 písm. a) bod 2 zákona č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente), ktorý zodpovedá úrovni bezpečnosti od zdokonaleného elektronického podpisu založenom na kvalifikovanom certifikáte (priamo zákon o e-Governmente posunul úroveň pre orgán verejnej moci na akceptovanie nižšej úrovne, ako je kvalifikovaný elektronický podpis, a teda orgán verejnej moci musí akceptovať všetky alternatívne formáty založené na kvalifikovanom certifikáte, čo znamená, že aj formát podpisu XAdES_ZEP.

V závislosti na odpovedi na 3b): Musí sa platnosť kvalifikovaného elektronického podpisu/pečate vytvorenej po 30. júni 2016 v profiloch XAdES_ZEP a CAdES_ZEP (ZEPf) vyhodnocovať v súlade s požiadavkami Nariadenia EP a Rady (EÚ) č. 910/2014? Alebo sa musí vyhodnocovať iba v súlade s pravidlami týchto profilov a prípadne aj v súlade s legislatívou účinnou do 30. júna 2016 na základe ktorej boli tieto profily vytvorené? Ktoré z týchto pravidiel majú prednosť pri vyhodnocovaní kvalifikovaného elektronického podpisu/pečate vytvoreného po 30. júni 2016?

Odpoveď na otázku je obsiahnutá vo vyššie uvedenom texte. Certifikát sa overuje cez TL a formát podpis na základe stavu, či orgán verejnej moci akceptuje aj formáty nižšej úrovne bezpečnosti ako kvalifikovaný elektronický podpis, kedy musí akceptovať aj alternatívne metódy, kam je možné XAdES_ZEP zaradiť.

Musí orgán verejnej moci používať na validovanie kvalifikovaného elektronického podpisu/pečate a časovej pečiatky vyhotovených do 1.7.2016 aplikácie uvedené NBÚ v zozname aplikácií pre vyhotovovanie a validovanie kvalifikovaného elektronického podpisu/pečate a časovej pečiatky certifikované na súlad s legislatívou platnou do 1. 7 .2016?

Formát podpisu XAdES_ZEP nie je nemožné vyžadovať a v prípade, ak sa dobrovoľne akceptuje, je potrebná špecifická aplikácia, ktorá spĺňa požiadavky uvedené vo formáte XAdES_ZEP, ktoré sú nad rámec prílohy Vykonávacieho rozhodnutia Komisie č. 2015/1506.

Ak sa orgán verejnej moci rozhodne akceptovať aj formáty kvalifikovaného elektronického podpisu (vyžadované legislatívou platnou do 1.7.2016) vyhotovené po 1.7.2016, musí použiť aplikáciu certifikovanú podľa nariadenia Európskeho parlamentu a Rady č. 910/2014, ktorá má certifikované aj formáty kvalifikované elektronické podpisy (vyžadované legislatívou platnou do 1. 7.2016)?

Nariadenie Európskeho parlamentu a Rady č. 910/2014 nevyžaduje certifikátu aplikácie, certifikáciu aplikácie vyžaduje len § 57e výnosu Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy v znení neskorších predpisov.

Čo to presne znamená, že aplikácia certifikovaná podľa nariadenia EP a Rady (EÚ) 910/2014 je zároveň certifikovaná pre formáty vyžadované do 30.6.2016, ktoré nie sú v súlade s týmto nariadením? Má takáto aplikácia uprednostňovať pravidlá vyplývajúce z Nariadenia 910/2014 pred pravidlami vyplývajúcimi zo špecifikácií daných formátov?

Formát podpisu XAdES_ZEP nie je možné vyžadovať od 01.07.2016 pre kvalifikovaný elektronický podpis a ak sa akceptuje orgánom verejnej moci, tak aplikácia musí nad rámec prílohy Vykonávacieho rozhodnutia Komisie č. 2015/1506 korektne vykonať obmedzenia a požiadavky definované vo formáte podpisu XAdES_ZEP.

S pozdravom

pplk. JUDr. Dušan Šnirc
riaditeľ